CLAIMS

What is claimed is:

1. A networking method comprising:

receiving descriptive data of networking traffic including timing data of the network traffic;

analyzing said timing data of the network traffic to determine whether the timing data is to be considered as an aberration; and

modifying the timing data if the timing data is to be considered as an aberration.

2. The method of claim 1, wherein said descriptive data of network traffic are network traffic flow oriented.

3. The method of claim 1, wherein said analyzing comprises comparing said timing data to timing patterns of previously received network traffic.

4. The method of claim 1, wherein said modifying comprises modifying said timing data to conform to timing patterns of earlier network traffic for which descriptive data were received.

5. The method of claim 4, wherein said method further comprises updating said timing patterns of earlier network traffic with said time data of the network traffic for which descriptive data was received.

6. The method of claim 5, wherein said updating of the timing patterns of earlier network traffic comprises weighing timing data of network traffic in a manner that biases towards the timing data of earlier network traffic over timing data of later network traffic.

7. An apparatus comprises:

storage medium having stored therein a plurality of programming instructions designed to implement a network traffic data collection function, when executed, enables the apparatus to

receive descriptive data of networking traffic including timing data of the network traffic,

analyze said timing data of the network traffic to determine whether the timing data is to be considered as an aberration, and

modify the timing data if the timing data is to be considered as an aberration; and

one or more processors coupled to the storage medium to execute the programming instructions.

8. The apparatus of claim 7, wherein said descriptive data of network traffic are network traffic flow oriented.

9. The apparatus of claim 7, wherein said network traffic collection function, when executed, enables said apparatus to perform said analyzing by comparing said timing data to timing patterns of previously received network traffic.

10. The apparatus of claim 7, wherein said network traffic collection function, when executed, enables said apparatus to perform said modifying by modifying said timing data to conform to timing patterns of earlier network traffic for which descriptive data were received.

11. The apparatus of claim 10, wherein said network traffic collection function, when executed, further enables said apparatus to update said timing patterns of earlier network traffic with said time data of the network traffic for which descriptive data was received.

12. The apparatus of claim 11, wherein said network traffic collection function, when executed, enables said apparatus to perform said updating of the timing patterns of earlier network traffic by weighing timing data of network traffic in a manner that biases towards the timing data of earlier network traffic over timing data of later network traffic.

13. A method comprising:

receiving a query to be run against a collection of network traffic data;

determining whether the query is to be run for a plurality of time bins;

determining said time bins if the query is to be run for a plurality of time bins; and

causing said query to be repeatedly run against said collection of network traffic data for said time bins using said generated looping instructions.

14. The method of claim 13, wherein said query comprises specifications for a start time for a first of said time bins, a number of time bins, and a stop time for a last

of said time bins; and said first and second determining as well as said generating are performed in accordance with said specifications.

15. The method of claim 14, wherein said number of time bins is explicitly specified.

16. The method of claim 15, wherein said number of time bins is implicitly specified through a specification of a time bin size, specified in conjunction with said start time of the first time bin, and said stop time of the last time.

17. The method of claim 13, wherein each of said repeated running of said query against said collection of network traffic data comprises automatically apportioning network traffic data between two time bins when the network traffic with which the network traffic data are associated straddles over the two time bins.

18. An apparatus comprising

storage medium having stored therein executable instructions designed to implement a network traffic data query facility, when executed, enables the apparatus to

receive a query to be run against a collection of network traffic data,

determine whether the query is to be run for a plurality of time bins,

determine said time bins if the query is to be run for a plurality of time bins, and

cause said query to be repeatedly run against said collection of network traffic data for said time bins using said generated looping instructions; and

one or more processors coupled to the storage medium to execute the instructions.

19. The apparatus of claim 18, wherein said query comprises specifications for a start time for a first of said time bins, a number of time bins, and a stop time for a last of said time bins; and said network traffic query facility, when executed, enables said apparatus to perform said first and second determining as well as said generating in accordance with said specifications.

20. The apparatus of claim 19, wherein said number of time bins is explicitly specified.

21. The apparatus of claim 19, wherein said number of time bins is implicitly specified through a specification of a time bin size, specified in conjunction with said start time of the first time bin, and said stop time of the last time.

22. The apparatus of claim 18, wherein said network traffic query facility, when executed, further enables the apparatus to automatically apportion network traffic data between two time bins when the network traffic with which the network traffic data are associated straddles over the two time bins, when running said query against said collection of network traffic data for one of said time bins.

23. A method comprising:

retrieving a record of network traffic data to be processed as part of an execution of a query against a collection of network traffic data comprising said record of network traffic data;

determining whether said record of network traffic data was created by its originating network trafficking device under a sampling mode;

determining a sampling ratio under which said record of network traffic data was created if said record of network traffic data was created by its originating network trafficking device under a sampling mode; and

amplifying one or more data elements of said retrieved record of network traffic data in accordance with said determined sampling ratio.

24. The method of claim 23, wherein said retrieved record of network traffic data comprises specifications for whether the record of network traffic data was created by its originating network trafficking device under a sampling mode, and if so, the sampling ratio; and said first and second determining are performed by analyzing said retrieved record of network traffic data.

25. An apparatus comprising

storage medium having stored therein executable instructions designed to implement a network traffic query facility, when executed, enables the apparatus to

retrieve a record of network traffic data to be processed as part of an execution of a query against a collection of network traffic data comprising said record of network traffic data,

determine whether said record of network traffic data was created by its originating network trafficking device under a sampling mode,

determine a sampling ratio under which said record of network traffic data was created if said record of network traffic data was created by its originating network trafficking device under a sampling mode, and

amplify one or more data elements of said retrieved record of network traffic data in accordance with said determined sampling ratio; and

one or more processors coupled to the storage medium to execute the instructions.

26. The apparatus of claim 25, wherein said retrieved record of network traffic data comprises specifications for whether the record of network traffic data was created by its originating network trafficking device under a sampling mode, and if so, the sampling ratio; and said network traffic data query facility, when executed, further enables the apparatus to perform said first and second determining by analyzing said retrieved record of network traffic data.

27. A method comprising:

receiving a query to be run against a collection of network traffic data;

determining if the query comprises a network traffic flow oriented command that specifies one or more processing to be performed for one or more network traffic flows;

determining said one or more processing to be performed for said one or more network traffic flows;

generating first byte codes for said one or more processing to be performed for said one or more network traffic flows; and

generating second byte codes to repeat execution of said first byte codes generated for said one or more processing for said one or more network traffic flows.

28. The method of claim 27, wherein said network traffic flow oriented command specifies said one or more processing are to be performed for each of said one or

more network traffic flows; and said second generating comprises generating said second byte codes which repeat execution of said first byte codes generated for said one or more processing for each of said one or more network traffic flows.

29. An apparatus comprising

storage medium having stored therein executable instructions designed to implement a network traffic data query facility, when executed, enables the apparatus to

receive a query to be run against a collection of network traffic data,

determine if the query comprises a network traffic flow oriented command that specifies one or more processing to be performed for one or more network traffic flows,

determine said one or more processing to be performed for one or more network traffic flows,

generate first byte codes for said one or more processing to be performed for one or more network traffic flows, and

generate second byte codes to repeat execution of said first byte codes generated for said one or more processing for one or more network traffic flows; and

one or more processors coupled to the storage medium to execute the instructions.

30. The apparatus of claim 29, wherein said network traffic flow oriented command specifies said one or more processing are to be performed for each of said one or more network traffic flows; and network traffic query facility, when executed, enables said apparatus to generate said second byte codes which repeat

execution of said first byte codes generated for said one or more processing for each of said one or more network traffic flows, when performing said second generating.

31. A method comprising:

receiving a query to be run against a collection of network traffic data;

determining if the query comprises a network traffic packet oriented command that specifies one or more processing to be performed for one or more network traffic packets;

determining said one or more processing to be performed for said one or more network traffic packets;

generating first byte codes for said one or more processing to be performed for said one or more network traffic packets; and

generating second byte codes to repeat execution of said first byte codes generated for said one or more processing for said one or more network traffic packets.

32. The method of claim 31, wherein said network traffic packet oriented command specifies said one or more processing are to be performed for a selected one of a first, a last and each of said one or more network traffic packets; and said second generating comprises a selected one of generating said second byte codes that execute said first byte code generated for said one more processor for a selected one of a first and a last of network traffic packets, and generating said second byte codes that repeat execution of said first byte codes generated for said one or more processing for each of said one or more network traffic packets.

33. An apparatus comprising

storage medium having stored therein executable instructions designed to implement a network traffic data query facility, when executed, enables the apparatus to

receive a query to be run against a collection of network traffic data,

determine whether the query comprises a network traffic packet oriented command that specifies one or more processing to be performed for one or more network traffic packets,

determine said one or more processing to be performed for said one or more network traffic packets,

generate first byte codes for said one or more processing to be performed for said one or more network traffic packets, and

generate second byte codes to repeat execution of said first byte code generated for said one or more processing for said one or more network traffic packets; and

one or more processors coupled to the storage medium to execute the instructions.

34. The apparatus of claim 33, wherein said network traffic packet oriented command specifies said one or more processing are to be performed for a selected one of a first, a last and each of said one or more network traffic packets; and said second generating comprises a selected one of generating said second byte codes that execute said first byte codes generated for said one more processor for a selected one of a first and a last of network traffic packets, and generating said second byte codes to repeat execution of said executable instructions generated for said one or more processing for each of said one or more network traffic packets.

35. A method comprising:

receiving a query to be run against a collection of network traffic data;

determining whether the query comprises a command;

determining whether the command comprises an expression;

determining whether the expression comprises one or more pre-determined network traffic attribute keywords; and

generating byte codes for said query, including byte codes for said command using said determined one or more pre-determined network traffic attribute keywords of said expression of said command.

36. The method of claim 35, wherein said one or more pre-determined network traffic attribute keywords comprise at least a selected one of a source address keyword, a destination address keyword, a next hop keyword, an ingress interface keyword, an egress interface keyword, a number of packets keyword, a number of byte keyword, a flow start time keyword, a flow end time keyword, a source port keyword, a destination port keyword, a TCP flag keyword, a protocol keyword, a type of service keyword, a source autonomous system keyword, a destination autonomous keyword, a source network address mask keyword, a destination network address mask keyword, and a number of network traffic flow keyword.

37. The method of claim 35, wherein said one or more pre-determined network traffic attribute keywords comprise at least a selected one of an original flow type keyword, a number of entries in a packet keyword, a router uptime keyword, a time keyword, an aggregation method keyword, an aggregation version keyword, a sampling interval keyword, and a sender address keyword.

38. An apparatus comprising

storage medium having stored therein executable instructions designed to implement a network traffic data query facility, when executed, enables the apparatus to

receive a query to be run against a collection of network traffic data;

determine whether the query comprises a command;

determine whether the command comprises an expression;

determine whether the expression comprises one or more pre-determined network traffic attribute keywords, and

generate byte codes for said query, including byte codes for said command using said determined one or more pre-determined network traffic attribute keywords of said expression of said command; and

one or more processors coupled to the storage medium to execute the instructions.

39. The apparatus of claim 38, wherein said one or more pre-determined network traffic attribute keywords comprise at least a selected one of a source address keyword, a destination address keyword, a next hop keyword, an ingress interface keyword, an egress interface keyword, a number of packets keyword, a number of byte keyword, a flow start time keyword, a flow end time keyword, a source port keyword, a destination port keyword, a TCP flag keyword, a protocol keyword, a type of service keyword, a source autonomous system keyword, a destination autonomous keyword, a source network address mask keyword, a destination network address mask keyword, and a number of network traffic flow keyword.

40. The apparatus of claim 38, wherein said one or more pre-determined network traffic attribute keywords comprise at least a selected one of an original flow type keyword, a number of entries in a packet keyword, a router uptime keyword, a time keyword, an aggregation method keyword, an aggregation version keyword, a sampling interval keyword, and a sender address keyword.